Federal Office
for Information Security

Common Criteria Protection Profile

Digital Tachograph – Smart Card (Tachograph Card)

Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10

BSI-CC-PP-0070

Version 1.02, 15th of November 2011

—— this page was intentionally left blank ——

Foreword

This Protection Profile (PP) 'Digital Tachograph - Smart Card (Tachograph Card)' has been developed to outline the IT security requirements as defined in the EU Commission Regulation 1360/2002, Annex I(B) [5], [6], Appendix 10 [8] (Tachograph Card Generic Security Target) in the Common Criteria (CC) language and format (CC version 3.1 [1], [2], [3], Revision 3). This is to enable developers of Tachograph Card products to build up their specific Security Target document according to CC in order to undergo a CC evaluation and certification process. The Tachograph Card product certificate is one pre-requisite to get the type approval of a Tachograph Card product.

The development of the PP has been sponsored by the Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany. The PP has been approved by the governmental IT security certification bodies organised within the Joint Interpretation Working Group (JIWG) which is supporting the mutual recognition of certificates under the umbrella of the European SOGIS-MRA (Agreement on Mutual Recognition of Information Technology Security Evaluation Certificates).

The PP continues the explicit intention of the European Commission to ensure a common and comparable level of assurance for the technical components of the Digital Tachograph System in Europe. As Appendix 10 [8] of the Commission Regulation mentioned above represents part of a legislative, this PP reflects the full content of the Tachograph Card Generic Security Target. It was not intended to modify or evolve the latter from a technical point of view. The coverage of the requirements of [8] by the CC Security Requirements defined in the current PP is stated in Annex A of this PP. The coverage of the assurance requirements as defined in [8] by this PP has been defined in a separate document (Joint Interpretation Library - Security Evaluation and Certification of Digital Tachographs) issued by the JIWG.

Correspondence and comments to this Protection Profile should be referred to:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 Bonn, Germany

Phone +49 228 99 9582-0
Fax +49 228 99 9582-5400

Email bsi@bsi.bund.de

—— this page was intentionally left blank ——

Contents

List of Tables

1 PP Introduction

1 This section provides document management and overview information required to register the Protection Profile and to enable a potential user of the PP to determine, whether the PP is of interest.

2 Requirements referred to in the present PP are those of the body of Annex I(B) of EU Commission Regulation 1360/2002 [5], [6]. For clarity of reading, duplication sometimes arises between Annex I(B) [5], [6] main body requirements and Protection Profile requirements. In case of ambiguity between a Protection Profile requirement and the Annex I(B) [5], [6] main body requirement referred by this Protection Profile requirement, the Annex I(B) main body requirement shall prevail.

3 Annex I(B) [5], [6] main body requirements not referred by this Protection Profile are not the subject of security certification.

4 Some security requirements of the PP are not included in the Generic Security Target (GST) [8] because it does not consider a smart card in general and incorporates only the extra security requirements needed by the tachograph application.

1.1 PP reference

5 The PP reference is given by:

Title	Common Criteria Protection Profile; Digital Tachograph — Smart Card (Tachograph Card)
Sponsor	Bundesamt für Sicherheit in der Informationstechnik
CC Version	3.1, Revision 3
Assurance Level	The assurance level for this PP is EAL4 augmented.
General Status	final version
Version Number	1.02
Registration	BSI-CC-PP-0070
Keywords	Digital Tachograph, Smart Card, 1360/2002 EC Annex I(B)

1.2 TOE Overview

1.2.1 TOE definition and operational usage

6 The Target of Evaluation (TOE) addressed by the current Protection Profile is a Tachograph Smart Card in the sense of Annex I(B) [5], [6] intended to be used in the Digital Tachograph System which contains additionally Motion Sensors and Vehicle Units as recording equipment.

7 A Tachograph Card is a smart card which comprises:

8 - the circuitry of the chip incl. all IC Dedicated Software (usually preloaded and often security certified by the Chip Manufacturer) being active in the operational phase of the TOE (the integrated circuit, IC),

9 - the IC Embedded Software (operating system, usually – together with IC – completely implementing executable functions),

10 - the tachograph application depending on the Tachograph Card type (driver card, workshop card, control card or company card) and

11 - the associated guidance documentation.

12 The basic functions of the Tachograph Card are:

13 - to store card identification and cardholder identification data. This data is used by the Vehicle Unit to identify the card holder, provide functions and data access rights accordingly, and ensure card holder accountability for his activities,

14 - to store cardholder activities data, events and faults data and control activities data, related to the cardholder.

15 A Tachograph Card is therefore intended to be used by a card interface device of a Vehicle Unit. It may also be used by any card reader (e.g. of a personal computer) if it has the appropriate access right.

16 Concerning the write access, during the end-usage phase of a Tachograph Card life-cycle (phase 7 of life-cycle as described in sec. 1.2.3 of this PP), only Vehicle Units may write user data to the card.

17 The functional requirements for a Tachograph Card are specified in Annex I(B) body text [5], [6] and Appendix 2 [7], the common security mechanisms are specified in Appendix 11 [9].

18 The Generic Security Target, Appendix 10 [8] requires that the TOE shall comply with PP/9806 [13] completely and with PP/9911 [14] as refined in [8] (see in particular subsections 4.2 – 4.9 of [8]). For the present PP, the following approach is chosen in accordance to JIL [10], sec. 2.3 and Annex C: This PP covers all aspects and

requirements defined in the PPs PP/9806 [13] and PP/9911 [14] but does not require CC conformance to these PPs. The coverage of [14] is reached through appropriate security functional and assurance requirements, all on the basis of the requirements and refinements outlined in [8], chap. 3 and 4. The compliance requirement related to [13] is replaced by the necessity of a CC conformance claim to the Security IC Platform Protection Profile [12]. The latter PP describes a comparable and acceptable set of (security) functionality for use as a basis for a Tachograph Card.

1.2.2 TOE major security features for operational use

19 The main security features of the TOE are as specified in [8]:

20
- The TOE must preserve card identification data and cardholder identification data stored during card personalisation process.

21
- The TOE must preserve user data stored in the card by Vehicle Units.

22 Specifically the Tachograph Card aims to protect

23
- the data stored in such a way as to prevent unauthorised access to and manipulation of the data and detecting any such attempts,

24
- the integrity and authenticity of data exchanged between the recording equipment and the Tachograph Card.

25 The main security features stated above are provided by the following major security services (please refer to [8], chap. 4):

26
- User and Vehicle Unit identification and authentication,

27
- Access control to functions and stored data,

28
- Accountability of stored data,

29
- Audit of events and faults,

30
- Accuracy of stored data,

31
- Reliability of services,

32
- Data exchange with a Vehicle Unit and export of data to a non-Vehicle Unit,

33
- Cryptographic support for ‘identification and authentication’ and ‘data exchange’ as well as for key generation and distribution in corresponding case according to [9], sec. 4.9.

34 All cryptographic mechanisms including algorithms and the length of corresponding keys have to be implemented exactly as required and defined in EU documents [8] and [9].

1.2.3 TOE Type

35 The TOE is a smart card, the Tachograph Card, which is configured and implemented as a driver card, workshop card, control card or company card in accordance with the specification documents Annex I(B) body text [5], [6], Appendix 2 [7], Appendix 10 [8] and Appendix 11 [9]. In particular, this implies the conformance with the following standards:

36 - ISO/IEC 7810 Identification cards – Physical characteristics

37 - ISO/IEC 7816 Identification cards - Integrated circuits with contacts:

38 - Part 1: Physical characteristics

39 - Part 2: Dimensions and location of the contacts

40 - Part 3: Electronic signals and transmission protocols

41 - Part 4: Inter-industry commands for interchange

42 - Part 8: Security related inter-industry commands

43 - ISO/IEC 10373 Identification cards – Test methods

44 As described in detail in the Security IC Platform Protection Profile [12], the typical smart card product life-cycle is decomposed in 7 phases as follows:

45 - Phase 1: Smart Card Embedded Software Development

46 - Phase 2: IC Design and IC Dedicated Software Development

47 - Phase 3: IC Manufacturing

48 - Phase 4: IC Packaging and Testing

49 - Phase 5: Smart Card Product Finishing Process

50 - Phase 6: Smart Card Personalisation

51 - Phase 7: Smart Card Product End-usage

52 The CC do not prescribe any specific life-cycle model. However, in order to define the application of the assurance classes, the CC assume the following implicit life-cycle model consisting of three phases:

53 - TOE development (including the development as well as the production of the TOE)

54 - TOE delivery

55 - TOE operational use

56 For the evaluation of the Tachograph card the phases 1 up to 4 as defined in [12] are part of the TOE development in the sense of the CC. The phase 7 - end-usage of the TOE is explicitly in focus of the current PP and is part of the operational use in the sense of the CC. The phases 5 and 6 may be part of one of these CC phases or may be split between them depending on the specific model used by the TOE Manufacturer[1]. The ST author shall define the exact boundary. However, this Protection Profile requires that the following conditions have to be met:

57 - All executable software in the TOE has to be covered by the evaluation.

58 - The data structures and the access rights to these data as defined in the Tachograph Card specification [7] in particular the initialisation file itself and its creation and handling are covered by the evaluation.

59 The phase 6 itself (Personalisation Phase) can be separated in two steps, the initialisation of the embedded software and personalisation of the end-user data, for short referred in the following as initialisation and personalisation. Concerning the functionality, the product (driver card, workshop card, control card or company card) is finished after initialisation, including creation of the application structure which implies:

60 - For file based operating systems: the creation of MF and corresponding DF(s)

61 - For JavaCard operating systems: the Applet instantiation.

62 But a TOE which is only initialised does not contain specific application data and is not ready for the end-usage phase. The product can be used as a Tachograph Card (driver card, workshop card, control card or company card) only after personalisation, in which application data including Tachograph Card specific cryptographic keys are stored.

63 As mentioned above the end-usage of the TOE is explicitly in focus of the current PP. Nevertheless, the Security Target authors have to define the TOE delivery exactly. The TOE delivery could take place before the initialisation and/or personalisation are finished. Depending on the TOE delivery concerning the life-cycle step the corresponding guidances for initialisation and/or personalisation as well as initialisation data have to be prepared and delivered too. It is assumed in this PP that the complete initialisation and personalisation activities will take place in secure environments.

64 The Security Target authors may extend the TOE security functionality with respect to initialisation and personalisation if these take place after delivery. If not and since the specific production steps of initialisation and/or personalisation are of major security relevance these have to be parts of the CC evaluation under ALC (see next application note). Nevertheless the decision about this has to be taken by the certification body. All production, generation and installation procedures after TOE

[1] Therefore in the remaining text of this PP the TOE Manufacturer will be the subject responsible for everything up to TOE delivery.

delivery up to the end-usage have to be considered in the product evaluation process under AGD assurance class.

65 The following examples and remarks may help ST authors to define the boundary of TOE development.

66 a) The following variations for the boundary of the TOE development are acceptable:

67 1. Phases 5 and 6 completely belong to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software, all data structures as defined in the Tachograph Card specification [7] and all card-specific data.

68 2. Phase 5 completely belongs to the TOE development, i.e. the TOE is delivered as an IC already embedded in the plastic card and containing all software and at least the data structures as defined in the Tachograph Card specification [7].

69 3. The TOE is delivered as an initialised module, i.e. it contains all software and at least the data structures as defined in the Tachograph Card specification [7], but isn't embedded in a plastic card yet.

70 4. The TOE is delivered in (at least) two parts: The hardware as a module or already embedded in a plastic card on the one hand and a file containing parts of the initialisation data (initialisation file) on the other hand. Both parts together again contain all software and at least the data structures as defined in the Tachograph Card specification [7] (which in particular means that all of this is evaluated during ADV activities). In this case the evaluation must also show as a result that the functions used by the customer (initialiser/personaliser/card issuer) for loading the initialisation data into the hardware provide sufficient protection against modification and (where applicable) disclosure of these data.

71 b) The following remarks may show how some CC assurance activities apply to parts of the life-cycle[2]:

72 1. The ALC class, which deals with security measures in the development environment of the TOE applies to all development and production environments of phases 1 up to 4 and those parts of phases 5 and 6 belonging to TOE development as defined in the ST for a TOE. In particular the sites, where the software of the TOE is developed as well as the hardware development and production sites are subject to this CC class (for example with regard to site visits). In the context of a composite evaluation some of the phases may already be covered by a IC hardware evaluation.

[2] These activities already follow from the CC definitions. Therefore it is not necessary to define them as refinements to the CC assurance components. However these explicit notes may serve as a help for ST writers and TOE developers to understand the connection between the life-cycle model and some CC requirements.

73 2. The measures for delivery of the TOE to the initialiser/personaliser/card issuer are subject to ALC_DEL.

74 3. If the fourth model described in "a." above is used (delivery of hardware and initialisation file), the loading of the initialisation data can be interpreted as part of installation and is therefore covered by assurance class ALC and ADV.

75 4. The guidance documentation delivered by the TOE developer as part of the TOE delivery procedures are covered by AGD_PRE. Since the initialiser/personaliser/card issuer is the first “user” of the TOE after delivery, the guidance documentation is mainly directed to him. He may be defined as the administrator of the TOE or as a special user role. Since the guidance documentation in particular needs to describe all measures necessary for secure use of the TOE, it needs to contain information on the following issues:

76 • Secure handling of the initialisation of the TOE including security measures needed for the initialisation and secure handling of the initialisation file.

77 • Secure handling of the personalisation of the TOE.

78 • Secure handling of delivery of the personalised TOE from the personaliser/card issuer to the cardholder.

79 • Security measures for end-usage, which the personaliser/card issuer needs to communicate to the cardholder. A simple example for this may be the requirement for the workshop card holder, to handle his PIN(s) securely. Since the documents accompanying the card during transport from card issuer to cardholder will probably not be available at the time of evaluation, the guidance documents for the personaliser/card issuer need to contain this information connected with the requirement that the card issuer covers all such issues in his delivery documents.

1.2.4 Required non-TOE hardware/software/firmware

80 The TOE is the Tachograph Card (contact based smart card). It is an independent product and does not need any additional hardware/software/firmware to ensure the security of the TOE.

81 In order to be powered up and to be able to communicate the TOE needs a card reader (integrated in the Vehicle Unit or connected to another device, e.g. a personal computer).

2 Conformance Claim

2.1 CC Conformance Claim

82 This Protection Profile claims conformance to

83
- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

84
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

85
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

as follows

86
- Part 2 extended,

87
- Part 3 conformant,

88 The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

has to be taken into account.

2.2 PP Claim

89 This PP does not claim any conformance to further Protection Profiles.

90 Although there is no PP to which the current PP is claimed to be conformant, this Tachograph Card PP covers all requirements of the Tachograph Card Generic ITSEC based ST as contained in [8]. The coverage of the requirements of [8] by the security functional requirements of the current PP is stated in Annex A, chap. 9 of this Protection Profile.

91 For the case of composite evaluation, the underlying integrated circuit of the TOE has to be successfully evaluated and certified in accordance with the Security IC Platform Protection Profile [12]. Otherwise all requirements of the Security IC Platform

Protection Profile [12] have to be integrated into the corresponding Tachograph Card Security Target.

2.3 Package Claim

92 The current PP is conformant to the following security requirements package:
– Assurance package E3hCC31_AP as defined in sec. 6.2 below. This assurance package is specified in dependence of JIL [10], Annex A, which defines a CC assurance package called E3hAP. The latter assurance package is intended to reach an equivalent assurance level in the framework of a CC certification as reached with an ITSEC E3 high certification (as required in [8]) and maps adequately (i.e. in particular in conjunction with the Digital Tachograph System) all assurance requirements from ITSEC E3 high into comparable CC requirements. Here, the assurance package E3hCC31_AP does not define a new security assurance level, but only directly switches the requirements in E3hAP, which are related to the older CC version 2.1 to the current version 3.1 of the CC ([3]).

93 The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5 (see sec. 6.2 below).

2.4 Conformance Claim Rationale

94 The current Protection Profile does not claim any conformance with other PPs. Therefore, no conformance claim rationale needs to be given here.

2.5 Conformance statement

95 This PP requires *strict* conformance of any ST or PP claiming conformance to this PP.

3 Security Problem Definition

96 *Application note 1*: Although each of the Tachograph Card types (driver card, workshop card, control card or company card) is used in different environment the author decided to describe the aspects of the Security Problem Definitions in general for the Tachograph Card considering the whole Digital Tachograph Systems and the corresponding usage of the Tachograph Cards.

3.1 Introduction

Assets

97 The assets to be protected by the TOE and its environment within phase 7 of the TOE's life-cycle are the application data defined as follows:

Object No.	Asset	Definition	Generic security property to be maintained by the TOE
1	Identification data (IDD)	Primary asset: card identification data, cardholder identification data (see Glossary for more details)	Integrity
2	Activity data (ACD)	Primary asset: cardholder activities data, events and faults data and control activity data (see Glossary for more details)	Integrity, Authenticity, for parts of the activity data also Confidentiality
3	Signature creation data (SCD)	Secondary asset: private key used to perform an electronic signature operation	Confidentiality, Integrity
4	Secret messaging keys (SMK)	Secondary asset: session keys (TDES) used to protect the Tachograph Card communication by means of secure messaging	Confidentiality, Integrity
5	Signature verification data (SVD)	Secondary asset: public keys certified by Certification Authorities, used to verify electronic signatures	Integrity, Authenticity
6	Verification authentication	Secondary asset: authentication data provided as input for authentication	Confidentiality (This security property is not

Object No.	Asset	Definition	Generic security property to be maintained by the TOE
	data (VAD)	attempt as authorised user (PIN)	maintained by the TOE but by the TOE environment)
7	Reference authentication data (RAD)	Secondary asset: data persistently stored by the TOE for verification of the authentication attempt as authorised user	Confidentiality, Integrity
8	Data to be signed (DTBS)	Secondary asset: the complete electronic data to be signed (including both user message and signature attributes)	Integrity, Authenticity
9	TOE File system incl. specific identification data	Secondary asset: file structure, access conditions, identification data concerning the IC and the Smartcard Embedded Software as well as the date and time of the personalisation	Integrity

Table 1: Assets to be protected by the TOE and its environment

98 All primary assets represent User Data in the sense of the CC. The secondary assets also have to be protected by the TOE in order to achieve a sufficient protection of the primary assets. The secondary assets represent TSF and TSF-data in the sense of the CC. The GST [8] defines “sensitive data” which include security data and user data as data stored by the Tachograph Card, which integrity, confidentiality and protection against unauthorised modification need to be enforced. User data include identification data and activity data (see Glossary for more details) and match User Data in the sense of the CC. Security data are defined as specific data needed to support security enforcement and match the TSF data in the sense of the CC.

Subjects and external entities

99 This Protection Profile considers the following subjects, who can interact with the TOE:

External Entity No.	Subject No.	Role	Definition
1	1	Administrator	S.Administrator: the subject is usually active only during Initialisation/Personalisation (Phase 6) – listed here for the sake of completeness.
2	2	Vehicle Unit	S.VU: Vehicle Unit (with a UserID), which the Tachograph Card is connected to.
3	3	Other devices	S.Non-VU: Other device (without UserID) which the Tachograph Card is connected to.
4	-	Attacker	It is a human or process acting on his behalf being located outside the TOE. For example, a driver could be an attacker if he misuses the driver card. An attacker is a threat agent (a person with the aim to manipulate the user data or a process acting on his behalf) trying to undermine the security policy defined by the current PP, especially to change properties of the maintained assets. The attacker is assumed to possess an at most *high* attack potential.

Table 2: Subjects and external entities

100 *Application note 2*: This table defines the subjects in the sense of [1] which can be recognised by the TOE independently of their nature (human or technical user). As result of an appropriate identification and authentication process, the TOE creates – for each of the respective external entities except the Attacker, who is listed for completeness – an 'image' inside and 'works' then with this TOE internal image (also called subject in [1]). From this point of view, the TOE itself does not distinguish between 'subjects' and 'external entities'.

101 *Application note 3*: The subject S.Administrator is not included in the security functional requirements because this PP describes the TOE only for the end-usage phase - after personalisation. The ST author may decide to include the personalisation process into the scope of the ST. In this case additional security functional requirements, which involve the subject S.Administrator, have to be included.

3.2 Threats

102 This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats are defined in reference to the according assets protected by the TOE and result from the method of TOE's use in the operational environment.

103 The following threats described also in GST [8], sec. 3.3.1 are defined in the current PP:

104 **T.Identification_Data** **Modification of Identification Data**

A successful modification of identification data held by the TOE (IDD, see sec. 3.1, e.g. the type of card, or the card expiry date or the cardholder identification data) would allow a fraudulent use of the TOE and would be a major threat to the global security objective of the system.

105 The threat agent for T.Identification_Data is Attacker.

106 **T.Activity_Data** **Modification of Activity Data**

A successful modification of activity data stored in the TOE (ACD, see sec. 3.1, e.g. cardholder activities data, events and faults data and control activity data) would be a threat to the security of the TOE.

107 The threat agent for T.Activity_Data is Attacker.

108 **T.Data_Exchange** **Modification of Activity Data during Data Transfer**

A successful modification of activity data (ACD deletion, addition or modification, see sec. 3.1) during import or export would be a threat to the security of the TOE.

109 The threat agent for T.Data_Exchange is Attacker.

110 The following additional threat related to the TOE's Personalisation Phase is supplemented:

111 **T.Personalisation_Data** **Disclosure or Modification of Personalisation Data**

A successful modification of personalisation data (such as TOE file system, cryptographic keys, RAD) to be stored in the TOE or disclosure of cryptographic material during the personalisation would be a threat to the security of the TOE. The threat addresses the execution of the TOE's personalisation process and its security.

112 The threat agent for T.Personalisation_Data is Attacker.

3.3 Organizational Security Policies

113 The TOE and/or its environment shall comply with the following Organisational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organisation upon its operation.

114 **P.EU_Specifications** **EU Specifications Conformance**

All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents [5] to [9]. To ensure the interoperability between the components all Tachograph Card and Vehicle Unit requirements concerning handling, construction and functionality inclusive the specified cryptographic algorithms and key length have to be fulfilled.

3.4 Assumptions

115 The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used.

116 **A.Personalisation_Phase Personalisation Phase Security**

All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation are correct according to the Tachograph Card Specification [7] and are handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys for the end-usage (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider controls all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE.

117 *Application note 4*: For the definition of the terms 'Personalisation Phase', 'initialisation' and 'personalisation' refer to sec. 1.2.3. Depending on the life-cycle model respective delivery model chosen for the TOE the assumption A.Personalisation_Phase has to be adapted appropriately (in particular in view of the security objective OE.Personalisation_Phase) by the ST author.

4 Security Objectives

118 This chapter describes the security objectives for the TOE and the security objectives for the TOE environment.

119 The security objectives for the TOE (OT) and the security objectives for the TOE environment (OE) will be defined in the following form

OT/OE.Name Short Title

Description of the objective.

4.1 Security Objectives for the TOE

120 This section describes the security objectives for the TOE, which address the aspects of identified threats to be countered by the TOE independently of the TOE environment and organizational security policies to be met by the TOE independently of the TOE environment.

121 The security objectives for the TOE are taken from the security objectives of GST [8], sec. 3.4 and sec. 3.5. The first two security objectives are directly derived from the overall security objective O.Main of the Digital Tachograph System (see [8], sec. 3.4), the following two security objectives cover specific IT security objectives intended to contribute to the main security objectives (see [8], sec. 3.5).

122 **OT.Card_Identification_Data Integrity of Identification Data**

The TOE must preserve card identification data and cardholder identification data stored during card personalisation process as specified by the EU documents [5] to [9].

123 **OT.Card_Activity_Storage Integrity of Activity Data**

The TOE must preserve user data stored in the card by Vehicle Units as specified by the EU documents [5] to [9].

124 **OT.Data_Access User Data Write Access Limitation**

The TOE must limit user data write access rights to authenticated Vehicle Units as specified by the EU documents [5] to [9].

125 **OT.Secure_Communications Secure Communications**

The TOE must be able to support secure communication protocols and procedures between the card and the card interface device when required by the application as specified by the EU documents [5] to [9].

4.2 Security Objectives for the Operational Environment

126 The security objectives for the TOE's operational environment address the security properties which have to be provided by the TOE environment independently of the TOE itself.

127 The TOE's operational environment has to implement security measures in accordance with the following security objectives:

128 **OE.Personalisation_Phase Secure Handling of Data in Personalisation Phase**

All data structures and data on the card produced during the Personalisation Phase, in particular during initialisation and/or personalisation must be correct according to the Tachograph Card Specification [7] and must be handled correctly regarding integrity and confidentiality of these data. This includes in particular sufficient cryptographic quality of cryptographic keys (in accordance with the cryptographic algorithms specified for Tachograph Cards) and their confidential handling. The Personalisation Service Provider must control all materials, equipment and information, which is used for initialisation and/or personalisation of authentic smart cards, in order to prevent counterfeit of the TOE. The execution of the TOE's personalisation process must be appropriately secured with the goal of data integrity and confidentiality.

129 For the definition of the terms 'Personalisation Phase', 'initialisation' and 'personalisation' refer to sec. 1.2.3. Depending on the life-cycle model respective delivery model chosen for the TOE the security objective OE.Personalisation_Phase for the operational environment of the TOE has to be adapted appropriately (in particular in view of the assumption A.Personalisation_Phase) by the ST author.

130 **OE.Tachograph_Components Implementation of Tachograph Components**

All Tachograph system components (Vehicle Unit, Motion Sensor and Tachograph Card) are specified by the EU documents [5] to [9]. To ensure the interoperability between the components all Vehicle Unit requirements concerning handling, construction and functionality inclusive the specified cryptographic algorithms and key length have to be fulfilled.

4.3 Security Objectives Rationale

131 The following table provides an overview for security objectives coverage (TOE and its environment) also giving an evidence for sufficiency and necessity of the security objectives defined. It shows that all threats are addressed by the security objectives for the TOE and that all OSPs are addressed by the security objectives for the TOE and its environment. It also shows that all assumptions are addressed by the security objectives for the TOE environment.

	Security objectives of the TOE	OT.Card_Identification_Data	OT.Card_Activity_Storage	OT.Data_Access	OT.Secure_Communications	**Security objectives of the TOE's operational environment**	OE.Personalisation_Phase	OE.Tachograph_Components
Threats								
T.Identification_Data		X						
T.Activity_Data			X	X				
T.Data_Exchange					X			
T.Personalisation_Data							X	
OSPs								
P.EU_Specifications		X	X	X	X			X
Assumptions								
A.Personalisation_Phase							X	

Table 3: Security Objective Rationale

132 A detailed justification required for suitability of the security objectives to cope with the security problem definition is given below.

133 **T.Identification_Data** is addressed by OT.Card_Identification_Data. The unalterable storage of personalised identification data of the TOE (cardholder identification data, card identification data) as defined in the security objective OT.Card_Identification_Data counters directly the threat T.Identification_Data.

134 **T.Activity_Data** is addressed by OT.Card_Activity_Storage and OT.Data_Access. The unalterable storage of Activity data as defined in the security objective OT.Card_Activity_Storage counters directly the threat T.Activity_Data. In addition, the security objective OT.Data_Access limits the user data write access to authenticated Vehicle Units so that the modification of activity data by regular card commands can be conducted only by authenticated card interface devices.

135 **T.Data_Exchange** is addressed by OT.Secure_Communications. The security objective OT.Secure_Communications provides the support for secure communication protocols and procedures between the TOE and card interface devices. This objective supports the securing of the data transfer between the TOE and card interface devices with the goal to prevent modifications during data import and export and counters directly the threat T.Data_Exchange.

136 **T.Personalisation_Data** is addressed by the security objective of the operational environment OE.Personalisation_Phase which requires correct and secure handling of the personalisation data regarding integrity and confidentiality. It prevents the modification and disclosure of the personalisation data as well as the disclosure of cryptographic material during the execution of the personalisation process.

137 The OSP **P.EU_Specifications** is covered by all objectives of the TOE and the objective for the environment OE.Tachograph_Components. The security objectives of the TOE OT.Card_Identification_Data, OT.Card_Activity_Storage, OT.Data_Access and OT.Secure_Communications require that the corresponding measures are implemented by the Tachograph Cards as specified by the EU documents. The objective for the environment OE.Tachograph_Components requires this for the Vehicle Unit.

138 The Assumption **A.Personalisation_Phase** is covered directly by the security objective of the operational environment OE.Personalisation_Phase. At this point, the focus of OE.Personalisation_Phase lies in the overall security of the personalisation environment and its technical and organisational security measures.

5 Extended Components Definition

139 This Protection Profile uses one component defined as extension to CC part 2. It is defined in the same way as in most smart card PPs, for example in the ICAO PP [15], registered and certified by BSI under the reference BSI-CC-PP-0056.

5.1 Definition of the Family FPT_EMS

140 The family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [2].

141 The family "TOE Emanation (FPT_EMS)" is specified as follows.

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE emanation
1

FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

6 Security Requirements

142 This part of the PP defines the detailed security requirements that shall be satisfied by the TOE. The statement of *TOE* security requirements shall define the *functional* and *assurance* security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE.

143 The CC allows several operations to be performed on security requirements (on the component level); *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 8.1 of Part 1 [1] of the CC. Each of these operations is used in this PP.

144 The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in **bold text** and changed words are ~~crossed out~~.

145 The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted by showing as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

146 The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are *italicised*. If the assignment made by the PP author defines a selection to be performed by the ST author, this text is underlined and italicised like *this*.

147 The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. In order to trace elements belonging to a component, the same slash "/" with iteration indicator is used behind the elements of a component.

6.1 Security Functional Requirements for the TOE

148 The security functional requirements (SFRs) below are derived from the security enforcing functions (SEFs) specified in chap. 4 of the ITSEC based Tachograph Card GST in [8]. Each of the SFRs includes in curly braces {…} a reference to the relevant SEFs (reference number or chapter of [8] resp. other documents). This not only explains why the given SFR has been chosen, but moreover is used to state further detail of the SFR without verbose repetition of the original text of the corresponding SEF(s) from [8]. The main advantage of this approach is avoiding redundancy, and, more important, any ambiguity.

149 The complete coverage of the security enforcing functions required in [8] is documented in Annex A, chap. 9 below.

6.1.1 Security Function Policy

150 The **Security Function Policy Access Control (AC_SFP)** for Tachograph Cards in the end-usage phase based on the Tachograph Cards Specification [7], sec. 3 and 4, GST [8], sec. 4.3.1 and 4.3.2 as well as JIL [10], sec. 2.6 is defined as follows:

151 The SFP AC_SFP is only relevant for the end-usage phase of the Tachograph Card, i.e. after the personalisation of the card has been completed.

152 Subjects:

153 - S.VU (in the sense of the Tachograph Card specification)

154 - S.Non-VU (other card interface devices)

155 Security attributes for subjects:

156 - USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)

157 - USER_ID Vehicle Registration Number (VRN) and Registering Member State Code (MSC), exists only for subject S.VU

158 Objects:

159 - user data:

160 - identification data (card identification data, cardholder identification data)

161 - activity data (cardholder activities data, events and faults data, control activity data)

162 - security data:

163 - cards´s private signature key

164 - public keys (in particular card´s public signature key; keys stored permanently on the card or imported into the card using certificates)

165 - session keys

166 - PIN (for workshop card only)

167 - TOE software code

168 - TOE file system (incl. file structure, additional internal structures, access conditions)

169 - identification data of the TOE concerning the IC and the Smartcard Embedded Software (indicated as identification data of the TOE in the following text)

170 - identification data of the TOE`s personalisation concerning the date and time of the personalisation (indicated as identification data of the TOE`s personalisation in the following text)

171 Security attributes for objects:

172 - Access Rules based on defined Access Conditions (see below) for:
    - user data
    - security data
    - identification data of the TOE
    - identification data of the TOE's personalisation

173 - Digital signature for each data to be signed

174 Operations:

175 - user data:

176
    - identification data: selecting (command Select), reading (command Read Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)

177
    - activity data: selecting (command Select), reading (command Read Binary), writing / modification (command Update Binary), download function (command Perform Hash of File, command PSO Compute Digital Signature)

178 - security data:

179
    - card´s private signature key: generation of a digital signature (command PSO Compute Digital Signature), internal authentication (command Internal Authenticate), external authentication (command External Authenticate)

180
    - public keys (in particular card´s public signature key): referencing over a MSE-command (for further usage within cryptographic operations as authentication, verification of a digital signature etc.)

181
    - session keys: securing of commands with Secure Messaging

182
    - PIN (only relevant for Workshop Card): verification (command Verify PIN)

183 - TOE software code: No Operations

184 - TOE file system (incl. file structure, additional internal structures, access conditions): No Operations

185 - identification data of the TOE: selecting and reading

186 - identification data of the TOE's personalisation (date and time of personalisation): selecting and reading.

187 **Access Rules:**

188 The SFP AC_SFP controls the access of subjects to objects on the basis of security attributes. The Access Condition (AC) defines the conditions under which a command executed by a subject is allowed to access a certain object. The possible commands are described in the Tachograph Card specification [7], sec. 3.6. Following Access Conditions are defined in the Tachograph Card specification [7], sec. 3.3:

189 - **NEV (Never)** - The command can never be executed.

190 - **ALW (Always)** - The command can be executed without restrictions.

191 - **AUT (Key based authentication)** - The command can be executed only if the preceding external authentication (done by the command External Authenticate) has been conducted successfully.

192 - **PRO SM (Secure Messaging providing data integrity and authenticity for command resp. response)** - The command can be executed and the corresponding response can be accepted only if the command/response is secured with a cryptographic checksum using Secure Messaging as defined in the Tachograph Card Specification [7], sec. 3.6 and Tachograph Common Security Mechanisms [9], sec. 5.

193 - **AUT and PRO SM** (combined, see description above)

194 For each type of Tachograph Card the Access Rules (which make use of the Access Conditions described above) for the different objects are implemented according to the requirements in the Tachograph Card Specification [7], sec. 4 and GST [8], sec. 4.3. These access rules cover in particular the rules for the export and import of data.

195 For the Tachograph Card type Workshop Card an additional AC is necessary. A mutual authentication process between the card and the external world is only possible if a successful preceding verification process with the PIN of the card has been taken place.

6.1.2 Class FAU Security Audit

FAU_SAA Security audit analysis

196 FAU_SAA.1 Potential Violation Analysis {chapter 4.5 of [8]}

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able **to detect failure events as cardholder authentication failures, self test errors, stored data integrity errors and activity data input integrity errors,**[3] to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of

- cardholder authentication failure,
- self test error,
- stored data integrity error,
- activity data input integrity error[4]

known to indicate a potential security violation;

b) [assignment: *any other rules*].

197 *Application Note 5*: The events cardholder authentication failure, self test error, stored data integrity error and activity data input integrity error may occur in combination or as single failure event.

6.1.3 Class FCO Communication

FCO_NRO Non-Repudiation of Origin

198 FCO_NRO.1 Selective proof of origin {chapter 4.8.2 of [8], DEX_304, DEX_305, DEX_306}

Hierarchical to: No other components.

[3] [refinement]

[4] [assignment: *subset of defined auditable events*]

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted data to be downloaded to external media[5] at the request of the recipient[6].

FCO_NRO.1.2 The TSF shall be able to relate the card holder identity by means of digital signature[7] of the originator of the information, and the hash value over the data to be downloaded to external media[8] of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to recipient[9] given in accordance with the Tachograph Common Security Mechanisms [9], sec. 6, CSM_035[10].

6.1.4 Class FCS Cryptographic support

FCS_CKM Cryptographic key management

199 FCS_CKM.1 Cryptographic key generation {chapter 4.9 of [8], CSP_301}

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm cryptographic two-keys TDES derivation algorithms[11] and specified cryptographic key sizes 128 bits with 112 effective bits[12] that meet the following: Tachograph Common Security Mechanisms [9], sec. 3, CSM_012, CSM_013, CSM_015, CSM_020[13].

[5] [assignment: *list of information types*]
[6] [selection: *originator, recipient, [assignment: list of third parties]*]
[7] [assignment: *list of attributes*]
[8] [assignment: *list of information fields*]
[9] [selection: *originator, recipient, [assignment: list of third parties]*]
[10] [assignment: *limitations on the evidence of origin*]
[11] [assignment: *cryptographic key generation algorithm*]
[12] [assignment: *cryptographic key sizes*]
[13] [assignment: *list of standards*]

200 FCS_CKM.2 Cryptographic key distribution {chapter 4.9 of [8], CSP_302}

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method TDES session key agreement by an internal-external authentication mechanism[14] that meets the following: Tachograph Common Security Mechanisms [9], sec. 3, CSM_012, CSM_013, CSM_015, CSM_020 and Tachograph Card Specification [7], sec. 3.6[15].

201 FCS_CKM.4 Cryptographic key destruction {chapter 4.9 of [8], CSP_301}

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: Tachograph Common Security Mechanisms [9], sec. 3, CSM_013 and Tachograph Card Specification [7], sec. 3.6[16].

202 *Application note 6*: As required in sec. 4.9 of [8] session keys shall have a limited (not more than 240) number of possible use. The ST authors have to consider the corresponding concrete number in FCS_CKM.1 and FCS_CKM.4 to fulfil the requirement CSM_013 in [9].

FCS_COP Cryptographic operation

203 FCS_COP.1/RSA Cryptographic operation {CSM_003 and further chapters of [9]}

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

[14] [assignment: *cryptographic key distribution method*]
[15] [assignment: *list of standards*]
[16] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ RSA The TSF shall perform the cryptographic operations (encryption, decryption, signature creation and signature verification as well as certificate verification for the authentication between the Tachograph Card and the Vehicle Unit and signing for downloading to external media)[17] in accordance with a specified cryptographic algorithm RSA[18] and cryptographic key sizes of 1024 bits[19] that meet the following: Tachograph Common Security Mechanisms [9], sec. 2-6, CSM_001, CSM_003, CSM_004, CSM_014, CSM_016, CSM_017, CSM_018, CSM_019, CSM_020, CSM_033, CSM_034, CSM_035 and Tachograph Card Specification [7], sec. 3[20].

204 FCS_COP.1/TDES Cryptographic operation {CSM_002 and further chapters of [9]}

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ TDES The TSF shall perform the cryptographic operations (encryption and decryption respective Retail-MAC generation and verification) concerning symmetric cryptography[21] in accordance with a specified cryptographic algorithm TDES[22] and cryptographic key sizes of 128 bits with 112 effective bits[23] that meet the following: Tachograph Common Security Mechanisms [9], sec. 2, CSM_005, sec. 3, CSM_015, sec. 5, CSM_021-CSM_031 and Tachograph Card Specification [7], sec. 3[24].

[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]
[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]

6.1.5 Class FDP User Data Protection

FDP_ACC Access control policy

205 FDP_ACC.2 Complete access control {chapter 4.3.1, ACT_301, ACT_302, chapter 4.4 of [8] as well as JIL [10], sec. 2.6}

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the AC_SFP[25] on

subjects:
- S.VU (in the sense of the Tachograph Card specification)
- S.Non-VU (other card interface devices)

objects:
- user data:
  - identification data
  - activity data
- security data:
  - cards´s private signature key
  - public keys
  - session keys
  - PIN (for workshop card)
- TOE software code
- TOE file system
- identification data of the TOE
- identification data of the TOE`s personalisation[26]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF Access control functions

206 FDP_ACF.1 Security attribute based access control {chapters 3.3 and 4 of [7], chapter 4.3.2, ACT_301, ACT_302, chapter 4.4 of [8] as well as JIL [10], sec. 2.6}

[25] [assignment: *access control SFP*]
[26] [assignment: *list of subjects and objects*]

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the AC_SFP[27] to objects based on the following:
subjects:

- S.VU (in the sense of the Tachograph Card specification)
- S.Non-VU (other card interface devices)

objects:

- user data:
    - identification data
    - activity data
- security data:
    - cards´s private signature key
    - public keys
    - session keys
    - PIN (for workshop card)
- TOE software code
- TOE file system
- identification data of the TOE
- identification data of the TOE`s personalisation

- security attributes for subjects:
    - USER_GROUP
    - USER_ID
- security attributes for objects:
    - Access Rules[28].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- GENERAL_READ:
    - driver card, workshop card: user data may be read from the TOE by any user

[27] [assignment: *access control SFP*]

[28] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

- control card, company card: user data may be read from the TOE by any user, except cardholder identification data which may be read by S.VU only;

- IDENTIF_WRITE: all card types: identification data may only be written once and before the end of Personalisation; no user may write or modify identification data during end-usage phase of card's life-cycle;

- ACTIVITY_WRITE: all card types: activity data may be written to the TOE by S.VU only;

- SOFT_UPGRADE: all card types: no user may upgrade TOE's software;

- FILE_STRUCTURE: all card types: files structure and access conditions shall be created before the Personalisation is completed and then locked from any future modification or deletion by any user

- IDENTIF_TOE_READ: all card types: identification data of the TOE and identification data of the TOE's personalisation may be read from the TOE by any user;

- IDENTIF_TOE_WRITE: all card types: identification data of the TOE may only be written once and before the Personalisation; no user may write or modify these identification data during the Personalisation;

- IDENTIF_ TOE_ PERS_WRITE: all card types: identification data of the TOE's personalisation may only be written once and within the Personalisation ; no user may write or modify these identification data during end-usage phase of card's life-cycle[29].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[30].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[31].

[29] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[30] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[31] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_DAU Data authentication

207 FDP_DAU.1 Basic Data Authentication {chapter 4.6.2 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of activity data[32].

FDP_DAU.1.2 The TSF shall provide S.VU and S.Non-VU[33] with the ability to verify evidence of the validity of the indicated information.

FDP_ETC Export from the TOE

208 FDP_ETC.1 Export of user data without security attributes {chapter 4.3.2 of [8]}

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the AC_SFP[34] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

209 FDP_ETC.2 Export of user data with security attributes {DEX_304, DEX_305, DEX_306, chapter 4.8 of [8]}

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1 The TSF shall enforce the AC_SFP[35] when exporting user data, controlled under the SFP(s), outside of the TOE.

[32] [assignment: *list of objects or information types*]

[33] [assignment: *list of subjects*]

[34] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

[35] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: none[36].

FDP_ITC Import from outside of the TOE

210 FDP_ITC.1 Import of user data without security attributes {chapters 4.3.1 and 4.3.2, RLB_305, chapter 4.7.2 of [8]}

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the AC_SFP[37] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none[38].

FDP_RIP Residual information protection

211 FDP_RIP.1 Subset residual information protection {RLB_306, RLB_307, chapter 4.7 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a

[36] [assignment: *additional exportation control rules*]
[37] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[38] [assignment: *additional importation control rules*]

resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

FDP_SDI Stored data integrity

212 FDP_SDI.2 Stored data integrity monitoring and action {chapter 4.6.1 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall warn the entity connected[39].

6.1.6 Class FIA Identification and Authentication

FIA_AFL Authentication failures

213 FIA_AFL.1/C Authentication failure handling {UIA_301, chapter 4.2.2 of [8], chapter 4.2.3 of [8]}

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/C The TSF shall detect when 1[40] unsuccessful authentication attempts occur related to authentication of a card interface device[41].

FIA_AFL.1.2/C When the defined number of unsuccessful authentication attempts has been met or surpassed[42], the TSF shall warn the entity

[39] [assignment: *action to be taken*]

[40] [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*]

[41] [assignment: *list of authentication events*]

[42] [selection: *met, surpassed*]

connected, assume the user as S.Non-VU[43].

214 FIA_AFL.1/WSC Authentication failure handling {UIA_302, chapter 4.2.2 of [8], chapter 4.2.3 of [8]}

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1/WSC The TSF shall detect when 5[44] unsuccessful authentication attempts occur related to PIN verification of Workshop Card[45].

FIA_AFL.1.2/WSC When the defined number of unsuccessful authentication attempts has been met or surpassed[46], the TSF shall warn the entity connected, block the PIN check procedure such that any subsequent PIN check attempt will fail, be able to indicate to subsequent users the reason of the blocking[47].

FIA_ATD User attribute definition

215 FIA_ATD.1 User attribute definition {chapter 4.2.1 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- USER_GROUP (VEHICLE_UNIT, NON_VEHICLE_UNIT)
- USER_ID (VRN and Registering MSC for subject S.VU)[48].

FIA_UAU User Authentication

216 FIA_UAU.1 Timing of authentication {UIA_301, chapter 4.2.2 of [8]}

Hierarchical to: No other components.

[43] [assignment: *list of actions*]
[44] [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*]
[45] [assignment: *list of authentication events*]
[46] [selection: *met, surpassed*]
[47] [assignment: *list of actions*]
[48] [assignment: *list of security attributes*]

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow

driver card, workshop card: export of user data with security attributes (card data download function),
control card, company card: export of user data without security attributes except export of cardholder identification data[49]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

217 FIA_UAU.3 Unforgeable authentication {UIA_301, chapter 4.2.2 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.3.1 The TSF shall prevent[50] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall prevent[51] use of authentication data that has been copied from any other user of the TSF.

218 FIA_UAU.4 Single-use authentication mechanisms {UIA_301, chapter 4.2.2 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to key based authentication mechanisms[52].

[49] [assignment: *list of TSF mediated actions*]
[50] [selection: *detect, prevent*]
[51] [selection: *detect, prevent*]
[52] [assignment: *identified authentication mechanism(s)*]

FIA_UID User identification

219 FIA_UID.1 Timing of identification {chapter 4.2.1 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow none of the TSF-mediated actions[53] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

220 *Application note 7*: The identification of the user is reached with the plug-in of the Tachograph Card into a card reader and the following power-up of the card.

FIA_USB User-subject binding

221 FIA_USB.1 User-subject binding {chapters 4.3.1, 4.7.2 (RLB_304, RLB_305) of [8]}

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- USER_GROUP (VEHICLE_UNIT for S.VU, NON_VEHICLE_UNIT for S.Non-VU)
- USER_ID (VRN and Registering MSC for subject S.VU)[54].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

[53] [assignment: *list of TSF-mediated actions*]
[54] [assignment: *list of user security attributes*]

6.1.7 Class FPR Privacy

FPR_UNO Unobservability

222 FPR_UNO.1 Unobservability {RLB_304, chapter 4.7.2 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNO.1.1 The TSF shall ensure that Attackers [55] are unable to observe the operation with involved authentication and/or cryptographic operations[56] on security and activity data[57] by any user[58].

6.1.8 Class FPT Protection of the TSF

FPT_EMS TOE Emanation

223 FPT_EMS.1 TOE Emanation {RLB_304, chapter 4.7.2 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [*assignment: types of emissions*] in excess of [assignment: *specified limits*] enabling access to private key(s) and session keys[59] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure any users[60] are unable to use the following interface smart card circuit contacts[61] to gain access to private key(s) and session keys[62] and [assignment: *list of types of user data*].

224 *Application note 8*: The ST writer shall perform the operation in FPT_EMS.1.1 and FPT_EMS.1.2. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical

[55] [assignment: *list of users and/or subjects*]
[56] [assignment: *list of operations*]
[57] [assignment: *list of objects*]
[58] [assignment: *list of protected users and/or subjects*]
[59] [assignment: *list of types of TSF data*]
[60] [assignment:: *type of users*]
[61] [assignment: *type of connection*]
[62] [assignment:: *list of types of TSF data*]

environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card.

FPT_FLS Fail secure

225 FPT_FLS.1 Failure with preservation of secure state {RLB_306, chapter 4.7.3, RLB_307, chapter 4.7.4 of [8]}

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: - reset - power supply cut-off - power supply variations - unexpected abortion of the TSF execution due to external or internal events (esp. break of a transaction before completion) [63].

FPT_PHP TSF physical protection

226 FPT_PHP.3 Resistance to physical attack {RLB_304, chapter 4.7.2 of [8]}

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing[64] to the all TOE components implementing the TSF[65] by responding automatically such that the SFRs are always enforced.

227 *Application note 9*: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSF security could not be violated at any time. Hence, “automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

[63] [assignment: *list of types of failures in the TSF*]
[64] [assignment: *physical tampering scenarios*]
[65] [assignment: *list of TSF devices/elements*]

FPT_TDC Inter-TSF TSF data consistency

228 FPT_TDC.1 Inter-TSF basic TSF data consistency {DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [8], chapter 5.3 of [9]}

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret key material (session keys and certificates)[66] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use rules for the interpretation of key material (session keys and certificates) as defined in Tachograph Common Security Mechanisms [9], and Tachograph Card Specification [7], sec. 3.6[67] when interpreting the TSF data from another trusted IT product.

FPT_TST TSF self test

229 FPT_TST.1 TSF testing {RLB_301, RLB_302, RLB_303, chapter 4.7.1 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests during initial start-up, periodically during normal operation[68] to demonstrate the correct operation of the TSF[69].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data[70].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of the TSF[71].

[66] [assignment: *list of TSF data types*]

[67] [assignment: *list of interpretation rules to be applied by the TSF*]

[68] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self test should occur]*]

[69] [selection: *[assignment: parts of TSF], the TSF*]

[70] [selection: *[assignment: parts of TSF data], TSF data*]

[71] [selection: *[assignment: parts of TSF], TSF*]

6.1.9 Class FTP Trusted path/channels

FTP_ITC Inter-TSF trusted channel

230 FTP_ITC.1 Inter-TSF trusted channel {DEX_301, DEX_302, DEX_303, chapter 4.8.1 of [8]}

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT product[72] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for activity data import from a remote trusted product[73].

6.2 Security Assurance Requirements for the TOE

231 The European Regulation [5], [6] requires for Tachograph Cards the assurance level ITSEC E3 high as specified in [8], chap. 6 and 7.

232 JIL [10], Annex A defines a CC assurance package called E3hAP. This assurance package is intended to reach an equivalent assurance level in the framework of a CC certification as reached with an ITSEC E3 high certification (as required in [8]) and maps adequately (i.e. in particular in conjunction with the Digital Tachograph System) all assurance requirements from ITSEC E3 high into comparable CC (version 2.1) requirements.

233 The current official CCMB version of Common Criteria is Version 3.1, Revision 3. This version defines in its part 3 assurance requirements components partially differing from the respective requirements of CC v2.x.

234 The CC community acts on the presumption that the EAL-Assurance Packages defined in CCv3.1 and CCv2.x are equivalent and can therefore be used for certification activities without restrictions.

[72] [selection: *the TSF, another trusted IT product*]

[73] [assignment: *list of functions for which a trusted channel is required*]

235 Based on these statements, an appropriate assurance package **E3hCC31_AP** as shown below was compiled and defined. The validity of this proposal is confined to the Digital Tachograph System. The assurance package E3hCC31_AP does not define a new security level, but only directly switches the requirements in E3hAP which are related to the older CC version 2.1 to the current version 3.1 of the CC ([3]).

Assurance Classes	**Assurance Family**	**E3hCC31_AP (based on EAL4)**
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_INT	-
	ADV_TDS	3
	ADV_SPM	-
Guidance Documents	AGD_OPE	1
	AGD_PRE	1
Life Cycle Support	ALC_CMC	4
	ALC_CMS	4
	ALC_DVS	1
	ALC_TAT	1
	ALC_DEL	1
	ALC_FLR	-
	ALC_LCD	1
Security Target evaluation	ASE	standard approach for EAL4
Tests	ATE_COV	2
	ATE_DPT	2
	ATE_FUN	1
	ATE_IND	2
AVA Vulnerability Assessment	AVA_VAN	5

Table 4: Assurance package E3hCC31_AP

236 The assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

237 *Application note 10:* The requirement {RLB_304} is partially covered by ADV_ARC (self-protection).

238 *Refinement 11*: The extent of the developer documentation and evidence related to the TOE depends on the point in time chosen for the TOE's delivery. The point in time for the TOE's delivery has a direct impact especially on the relevant assurance families resp. classes ASE, AGD and ATE. The evaluation body has to examine that the developer documentation and evidence matches the delivery model chosen for the TOE.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

239 The following table shows, which SFRs for the TOE support which security objectives of the TOE. The table shows, that every objective is supported by at least one SFR and that every SFR supports at least one objective.

	OT.Card_ Identification_ Data	**OT.Card_ Activity_Storage**	**OT.Data_Access**	**OT.Secure_ Communications**
FAU_SAA.1	X	X		X
FCO_NRO.1				X
FCS_CKM.1				X
FCS_CKM.2				X
FCS_CKM.4				X
FCS_COP.1/RSA				X
FCS_COP.1/TDES				X
FDP_ACC.2	X	X	X	X
FDP_ACF.1	X	X	X	X
FDP_DAU.1				X
FDP_ETC.1				X
FDP_ETC.2				X
FDP_ITC.1				X
FDP_RIP.1				X
FDP_SDI.2	X	X		
FIA_AFL.1/C			X	
FIA_AFL.1/WSC			X	
FIA_ATD.1			X	
FIA_UAU.1			X	
FIA_UAU.3			X	X
FIA_UAU.4				X
FIA_UID.1			X	
FIA_USB.1			X	

	OT.Card_ Identification_ Data	OT.Card_ Activity_Storage	OT.Data_Access	OT.Secure_ Communications
FPR_UNO.1				X
FPT_EMS.1	X	X	X	X
FPT_FLS.1	X	X	X	X
FPT_PHP.3	X	X	X	X
FPT_TDC.1				X
FPT_TST.1	X	X	X	X
FTP_ITC.1				X

Table 5: Coverage of Security Objectives for the TOE by SFRs

240 A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

241 According to the security objective **OT.Card_Identification_Data**, the TOE preserves card identification data and cardholder identification data stored during card personalisation process as specified by the EU documents. The access to the TOE's data, especially to the identification data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1, explicitly denies the write access to personalised identification data. The integrity of the stored data within the TOE, especially the integrity of the identification data is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1 (as single failure event or in combination with other failure events), the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the stored identification data and their modification.

242 According to the security objective **OT.Card_Activity_Storage**, the TOE preserves user data stored in the card by Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1. This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1, explicitly restricts the write access to user data to authenticated Vehicle Units. The integrity of the stored data within the TOE, especially the integrity of the user data written by Vehicle Units is secured by the component FDP_SDI.2. In case of an integrity error detected by the component FAU_SAA.1, the TOE will indicate the corresponding violation. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the user data written by Vehicle Units and their modification.

243 According to the security objective **OT.Data_Access**, the TOE limits the user data write access in the TOE's end-usage phase to authenticated Vehicle Units as specified by the EU documents. The access to the TOE's data, especially to the user data is regulated by the security function policy AC_SFP as defined in chap. 6.1.1.

This SFP, accomplished by the components FDP_ACC.2 and FDP_ACF.1,explicitly restricts the write access to user data to authenticated Vehicle Units. The components FIA_USB.1 and FIA_ATD.1 with its definition of the user security attributes supply a distinction between Vehicle Units and other card interface devices. The components FIA_UID.1 and FIA_UAU.1 ensure that especially the write access to user data is not possible without a preceding successful authentication process. If the authentication fails, the component FIA_AFL.1/C resp. FIA_AFL.1/WSC reacts with a warning to the connected entity, and the user will be assumed as different from a Vehicle Unit. The component FIA_UAU.3 prevents the use of forged authentication data. Finally, the components FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to user data write access.

244 According to the security objective **OT.Secure_Communication**, the TOE supports secure communication protocols and procedures between the card and the card interface device when required by the application as specified by the EU documents.

245 The component FTP_ITC.1 together with FDP_ETC.1 and FDP_ITC.1 offers the possibility to secure the data exchange (i.e. the data import and export) between the TOE and the card interface device by using a trusted channel assuring identification of its end points and protection of the data transfer from modification and disclosure. Hereby, both parties are capable of verifying the received data with regard to their integrity and authenticity. The trusted channel assumes a successful preceding mutual key based authentication process between the TOE and the card interface device with agreement of session keys which is covered by the components FCS_CKM.1, FCS_CKM.2, FCS_CKM.4 and FCS_COP.1/RSA for cryptographic support. The cryptographic component FCS_COP.1/TDES realise the securing of the data exchange itself. The components FPR_UNO.1 guarantees for the unobservability of the establishing process of the trusted channel and for the unobservability of the data exchange itself which both contributes to a secure data transfer. The components FIA_UAU.3 and FIA_UAU.4 support the security of the trusted channel as the TOE prevents the use of forged authentication data and as the TOE’s input for the authentication tokens and for the session keys within the preceding authentication process is used only one time. During data exchange, upon detection of an integrity error of the imported data, the TOE will indicate the corresponding violation and will send a warning to the entity sending the data, which is realised by the component FAU_SAA.1.

246 Furthermore, within the TOE’s end-usage phase, the TOE offers a data download functionality with specific properties. The TOE provides the capability to generate an evidence of origin for the data downloaded to the external media, to verify this evidence of origin by the recipient of the data downloaded and to download the data to external media in such a manner that the data integrity can be verified. All these requirements are covered by FDP_ETC.2, FCO_NRO.1 and FDP_DAU.1. The corresponding cryptographic components for conducting the data download process with its security features are given with FCS_COP.1/RSA.

247 For each secure communication described above, the component FPT_TDC.1 ensures for a consistent interpretation of the security related data shared between the TOE and the external world. The necessity for the usage of a secure communication protocol as well as the access to the relevant card´s keys is deposited in the security

function policies AC_SFP defined in chap. 6.1.1. These policies correspond directly to the SFRs FDP_ACC.2 and FDP_ACF.1. Finally, the components FDP_RIP.1, FPT_EMS.1, FPT_FLS.1, FPT_PHP.3 and FPT_TST.1 support the correct and secure operation of the TOE with regard to the secure communication protocols.

6.3.2 SFR Dependency Rationale

248 The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed, and non-dissolved dependencies are appropriately explained.

249 The table below shows the dependencies between the SFR of the TOE.

SFR	Dependencies	Support of the Dependencies
FAU_SAA.1	FAU_GEN.1 Audit data generation	justification 1 for non-satisfied dependencies
FCO_NRO.1	FIA_UID.1 Timing of identification	FIA_UID.1
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.2, FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1
FCS_COP.1/RSA	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	justification 2 for non-satisfied dependencies
FCS_COP.1/TDES	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or	

SFR	Dependencies	Support of the Dependencies
	FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1, FCS_CKM.4
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation	FDP_ACC.2, justification 3 for non-satisfied dependencies
FDP_DAU.1	No dependencies	-
FDP_ETC.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	FDP_ACC.2
FDP_ETC.2	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]	FDP_ACC.2
FDP_ITC.1	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.2, justification 3 for non-satisfied dependencies
FDP_RIP.1	No dependencies	-
FDP_SDI.2	No dependencies	-
FIA_AFL.1/C	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_AFL.1/WSC	FIA_UAU.1 Timing of authentication	FIA_UAU.1
FIA_ATD.1	No dependencies	-
FIA_UID.1	No dependencies	-
FIA_UAU.1	FIA_UID.1 Timing of identification	FIA_UID.1
FIA_UAU.3	No dependencies	-
FIA_UAU.4	No dependencies	-
FIA_UID.1	No dependencies	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FPR_UNO.1	No dependencies	-
FPT_EMS.1	No dependencies	-
FPT_FLS.1	No dependencies	-
FPT_PHP.3	No dependencies	-
FPT_TDC.1	No dependencies	-
FPT_TST.1	No dependencies	-
FTP_ITC.1	No dependencies	-

Table 6: Dependency rationale overview

250 Justification for non-satisfied dependencies:

251 No.1: The dependency FAU_GEN.1[74] (Audit Data Generation) is not applicable to the TOE. Tachograph cards do not generate an audit record but reacts with an error response resp. reset. The detection of failure events implicitly covered in FAU_SAA.1 is clarified by a related refinement of the SFR.

252 No.2: The SFR FCS_COP.1/RSA uses keys which are loaded or generated during the personalisation and are not updated or deleted over the life time of the TOE. Therefore none of the listed SFR are needed to be defined for this specific instantiations of FCS_COP.1/RSA.

253 No.3: The access control TSF according to FDP_ACF.1 uses security attributes (access rules, refer to sec. 6.1.1) which are defined during the Personalisation Phase respective initialisation (for the terms refer to sec. 1.2.3) and are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here, neither during the personalisation nor within the usage phase of the TOE. This argument holds for FDP_ACF.1 as well as for FDP_ITC.1.

6.3.3 Security Assurance Requirements Rationale

254 The current protection profile is claimed to be conformant with the assurance package E3hCC31_AP (cf. sec. 2.3 above). As already mentioned in sec. 6.2, the assurance package E3hCC31_AP represents the standard assurance package EAL4 augmented by the assurance components ATE_DPT.2 and AVA_VAN.5.

255 The main reason for the choice of the package E3hCC31_AP is the legislative framework [10], where the assurance level required is defined in form of the assurance package E3hAP (for CCv2.1). The author only translated this assurance package E3hAP into the assurance package E3hCC31_AP in accordance with the current version 3.1 of the CC ([3]). These packages are commensurate with each other.

256 The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

[74] The FAU_GEN.1 component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable in a smart card since many of these events indicate an insecure card state where recording of the event itself could cause a security breach.

257 The selection of the component ATE_DPT.2 provides a higher assurance than the pre-defined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

258 The selection of the component AVA_VAN.5 provides a higher assurance than the pre-defined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential (see also Table 2: Subjects, entry 'Attacker'). This decision represents a part of the conscious security policy for the Tachograph Cards required by the legislative [5], [6] and reflected by the current PP.

259 The set of assurance requirements being part of EAL4 fulfils all dependencies a priori.

260 The augmentation of EAL4 chosen comprises the following assurance components:

261 - ATE_DPT.2 and

262 - AVA_VAN.5.

263 For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package:

Component	Dependencies required by CC Part 3 or ASE_ECD	Dependencies fulfilled by
ATE_DPT.2	ADV_ARC.1	ADV_ARC.1
	ADV_TDS.3	ADV_TDS.3
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.5	ADV_ARC.1	ADV_ARC.1
	ADV_FSP.4	ADV_FSP.4
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_DPT.1	ATE_DPT.2

Table 7: SAR Dependencies

264 The refinement added to the chosen SAR package (refer to sec. 6.2) addresses the flexibility of the PP related to the TOE's delivery. In dependency of the chosen point in time for the TOE's delivery, the developer documentation and evidence has to be set-up appropriately and the evaluation body is in charge of examining the provided developer evidence for suitability in relationship to the TOE's delivery model.

6.3.4 Security Requirements – Internal Consistency

265 The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together form an internally consistent whole.

a) SFRs

266 The dependency analysis in section 6.3.2 SFR Dependency Rationale for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.

267 All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items. Furthermore, the current PP accurately and completely reflects the Generic Security Target [8]. Since the GST [8] is part of the related legislation, it is assumed to be internally consistent. Therefore, due to conformity between the current PP and [8], also subjects and objects being used in the current PP are used in a consistent way.

b) SARs

268 The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 Security Assurance Requirements Rationale shows that the assurance requirements are internally consistent, because all (additional) dependencies are satisfied and no inconsistency appears.

269 Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met – an opportunity having been shown not to arise in sections 6.3.2 SFR Dependency Rationale and 6.3.3 Security Assurance Requirements Rationale. Furthermore, as also discussed in section 6.3.3 Security Assurance Requirements Rationale, the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 Glossary and Acronyms

Glossary

Term	Definition
Activity data	Activity data include user activities data, events and faults data and control activity data (date and time of first use of the vehicle, vehicle odometer value at that time, date and time of last use of the vehicle, vehicle odometer value at that time, VRN and registering Member State of the vehicle, date and time the session was opened, a daily presence counter, the total distance travelled by the driver during this day, a driver status at 00.00, information about changed activity, data related to places where daily work periods begin and/or end (the date and time of the entry, the type of entry, the country and region entered, the vehicle odometer value), records of calibrations and/or time adjustments performed as well as counter indicating the number of calibrations performed (workshop card), date and time of the control, type of the control, period downloaded (control card), date and time of the activity, type of the activity, period downloaded (company card)).
Application note	Optional informative part of the PP containing sensible supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.
Authenticity	Ability to confirm that an entity itself and the data elements stored in were issued by the entity issuer
Cardholder	The rightful/legitimated holder of the Tachograph Card.
Certificate chain	Hierarchical sequence of Equipment Certificate (lowest level), Member State Certificate and European Public Key (highest level), where the certificate of a lower lever is signed with the private key corresponding to the public key in the certificate of the next higher level.
Certification authority	A natural or legal person who certifies the assignment of public keys (for example PK.EQT) to serial number of equipment and to this end holds the licence.
Digital Signature	A digital signature is a seal affixed to digital data which is generated by the private signature key of an entity (a private signature key) and establishes the owner of the signature key (the

	entity) and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority.
Digital Tachograph	Recording equipment including a Vehicle Unit and a motion sensor connected to it.
Digital Tachograph System	Equipment, people or organisations, involved in any way with the recording equipment and Tachograph Cards.
IC Dedicated Software	Software developed and injected into the chip hardware by the IC manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players.
IC Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
Identification data	Identification data includes Card identification data (tachograph application data, type of Tachograph Card, IC serial number, IC manufacturing references, card number, card type approval number, card personalisation identification, issuing Member state, issuing authority name, issue date, card beginning of validity date, card expire date) and Cardholder identification data (surname and first name, date of birth, preferred language, issuing Member State, issuing authority name, driving licence number, workshop name and address (workshop card), control body name and address (control card), company name and address (company card)).
Initialisation	The process by which the card-specific structure data and non-card-specific data are stored in the card: for file based operating systems - the creation of MF and corresponding DF(s); for JavaCard operating systems - the Applet instantiation.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions. Tachograph Card's chip is an IC.
Motion data	The data exchanged with the Vehicle Unit, representative of speed and distance travelled.
Personal Identification Number (PIN)	A short secret password being only known to the approved workshops, necessary for using of workshop cards.

Personalisation	The process by which the card-specific data and individual-related data (inclusive the cryptographic keys) are stored in the card.
Personalisation data	The card-specific and individual-related data inclusive the cryptographic keys stored during the Personalisation.
Personalisation Phase	The personalisation phase (Phase 6 of the IC life-cycle) includes the initialisation as well as the personalisation.
Pre-Personalisation	The process by which the chip-specific data are stored in the non-volatile memory of the TOE by the Chip Manufacturer for traceability of the non-personalised Cards and/or to secure shipment within or between the life-cycle phases. During the Pre-Personalisation the non-card-specific data (for example patch code) could be loaded too.
Security data	The specific data needed to support security enforcing functions (e.g. cryptographic keys), see sec. III.12.2 of [5]. Security data are part of sensitive data.
Sensitive data	Data stored by the recording equipment and by the Tachograph Cards that need to be protected for integrity, unauthorised modification and confidentiality (where applicable for security data). Sensitive data includes security data and user data.
Tachograph cards	Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A Tachograph Card may be of the following types: driver card, control card, workshop card, company card.
TSF data	Data created by and for the TOE that might affect the operation of the TOE (CC part 1 [1]).
User Data	Any data, other than security data (sec. III.12.2 of [5]) and authentication data, recorded or stored by the VU, required by Chapter III.12 of the Commission Regulation [5]. User data are part of sensitive data. CC give the following generic definitions for user data: Data created by and for the user that does NOT affect the operation of the TSF (CC part 1 [1]). Information stored in TOE resources that can be operated upon by users in accordance with the SFRs and

	upon which the TSF places no special meaning (CC part 2 [2]).
Vehicle Unit	The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The Vehicle Unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.
Verification data	Data provided by an entity in an authentication attempt to prove their identity to the verifier. The verifier checks whether the verification data match the reference data known for the claimed identity.

Acronyms

Acronym	Term
AC	Access Condition
ACD	Activity Data
CBC	Cipher Block Chaining
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
DF	Dedicated File
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
GST	Generic Security Target for Tachograph Card as defined in [8]
IDD	Identification Data
ICV	Initial Chaining Value
MAC	Message Authentication Code
MF	Master File
MSC	Member State Certificate
PP	Protection Profile
PIN	Personal Identification Number
RAD	Reference Authentication Data
SAR	Security Assurance Requirement
SCD	Signature Creation Data

SFR	Security Functional Requirement
SM	Secure Messaging
SMK	Secret Messaging Keys
SVD	Signature Verification Data
TOE	Target Of Evaluation
TDES	Triple DES
TSF	TOE Security Functionality
VAD	Verification Authentication Data
VRN	Vehicle Registration Number
VU	Vehicle Unit

8 Literature

Common Criteria

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

Digital Tachograph: Directives and Standards

[5] Annex I(B) of Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)

[6] Corrigendum to Commission Regulation (EC) No. 1360/2002 of 13 June 2002 adapting for the seventh time to technical progress Council Regulation (EEC) No. 3821/85 on recording equipment in road transport, Official Journal of the European Communities L 71-86, 13.03.2004

[7] Appendix 2 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] – Tachograph Cards Specification

[8] Appendix 10 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] - Generic Security Targets

[9] Appendix 11 of Annex I(B) of Commission Regulation (EEC) No. 1360/2002 [5] - Common Security Mechanisms

[10] Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1(B), Version 1.12, June 2003

[11] RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003

[12] Security IC Platform Protection Profile, BSI-CC-PP-0035, Version 1.0, June 2007; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0035-2007

[13] Smartcard Integrated Circuit Protection Profile - version 2.0 - issue September 1998. Registered at French certification body under the number PP/9806

[14] Smartcard Integrated Circuit With Embedded Software Protection Profile - version 2.0 - issue June 1999. Registered at French certification body under the number PP/9911

[15] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application”, Extended Access Control, Version 1.10, 25th March 2009; registered and certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-CC-PP-0056

9 Annex A: Coverage of the GST Requirements

270 GST [8] contains in sec. 4 the description of the the security enforcing functions for the Tachograph Cards. This Annex A is only informative and maps each statement from the sec. 4 of GST [8] to the relevant SFR of the current PP and gives the evidence that all required security enforcing functions are considered in the PP. The SFR descriptions (if needed) contain the relevant references to the Tachograph Cards Specification [7] which defines the functionality inclusive the access conditions as well as the relevant references to the Common Security Mechanisms [9] to be used. Some SFRs refer the JIL [10] which contains clarifications concerning the Tachograph Cards functionality.

271 The following table demonstrates the coverage of the requirements of [8], chapter 4 by the security functional requirements chosen in the current PP and specified in section 6.1 'Security Functional Requirements for the TOE' above.

Requirement, Appendix 10, [8]	Requirement Description, Appendix 10, [8]	Related statement in the current PP
Chapter 4.1	**Compliance to Protection Profiles**	
CPP_301	The TOE shall comply with (IC PP).	PP BSI-PP-0035 (see sec. 1.2.1)
CPP_302	The TOE shall comply with (ES PP) as refined further.	sec. 6.1
Chapter 4.2	**Identification & Authentication**	
Chapter 4.2 Chapter 4.2.1	The card must identify the entity in which it is inserted and know whether it is an authenticated Vehicle Unit or not. The card may export any user data whatever the entity it is connected to, except the control card which may export card holder identification data to authenticated Vehicle Units only (such that a controller is ensured that the Vehicle Unit is not a fake one by seeing his name on display or printouts). Assignment (FIA_UID.1.1) List of TSF mediated actions: none. Assignment (FIA_ATD.1.1) List of security attributes: USER_GROUP VEHICLE_UNIT, NON_VEHICLE_UNIT, USER_ID Vehicle Registration Number (VRN) and registering Member State Code (USER_ID is known for USER_GROUP = VEHICLE_UNIT only).	FIA_UID.1 FIA_ATD.1

Chapter 4.2.2	Assignment (FIA_UAU.1.1) List of TSF mediated actions: - Driver and Workshop cards: export user data with security attributes (card data download function), - Control card: export user data without security attributes except cardholder identification data.	FIA_UAU.1
UIA_301	Authentication of a Vehicle Unit shall be performed by means of proving that it possesses security data that only the system could distribute. Selection (FIA_UAU.3.1 and FIA_UAU.3.2): prevent. Assignment (FIA_UAU.4.1) Identified authentication mechanism(s): any authentication mechanism.	FIA_UAU.1, FIA_UAU.3 FIA_UAU.4 FIA_AFL.1/C
UIA_302	The Workshop card shall provide an additional authentication mechanism by checking a PIN code (This mechanism is intended for the Vehicle Unit to ensure the identity of the card holder, it is not Intended to protect workshop card content).	FIA_AFL.1/WSC
Chapter 4.2.3	The following assignments describe the card reaction for each single user authentication failure. Assignment (FIA_AFL.1.1) Number: 1, list of authentication events: authentication of a card interface device. Assignment (FIA_AFL.1.2) List of actions: - warn the entity connected, - assume the user as NON_VEHICLE_UNIT. The following assignments describe the card reaction in the case of failure of the additional authentication mechanismrequired in UIA_302. Assignment (FIA_AFL.1.1) Number: 5, list of authentication events: PIN checks (workshop card). Assignment (FIA_AFL.1.2) List of actions: - warn the entity connected, - block the PIN check procedure such that any subsequent PIN check attempt will fail, - be able to indicate to subsequent users the reason of the blocking.	FIA_AFL.1/C, FIA_AFL.1/WSC
Chapter 4.3	**Access Control**	
Chapter 4.3.1	During end-usage phase of its life-cycle, the Tachograph Card is the subject of one single access	FDP_ACC.2 FIA_USB.1

	control security function policy (SFP) named AC_SFP. Assignment (FDP_ACC.2.1) Access control SFP: AC_SFP.	FDP_ITC.1
Chapter 4.3.2	Assignment (FDP_ACF.1.1) Access control SFP: AC_SFP. Assignment (FDP_ACF.1.1) Named group of security attributes: USER_GROUP. Assignment (FDP_ACF.1.2) Rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects: GENERAL_READ: User data may be read from the TOE by any user, except cardholder identification data which may be read from control cards by VEHICLE_UNIT only. IDENTIF_WRITE: Identification data may only be written once and before the end of phase 6 of card's life-cycle. No user may write or modify identification data during end-usage phase of card's life-cycle. ACTIVITY_WRITE: Activity data may be written to the TOE by VEHICLE_UNIT only. SOFT_UPGRADE: No user may upgrade TOE's software. FILE_STRUCTURE: Files structure and access conditions shall be created before end of phase 6 of TOE's life-cycle and then locked from any future modification or deletion by any user.	FDP_ACF.1 FDP_ETC.1 FDP_ITC.1
Chapter 4.4	**Accountability**	
ACT_301	The TOE shall hold permanent identification data.	FDP_ACC.2 FDP_ACF.1
ACT_302	There shall be an indication of the time and date of the TOE's personalisation. This indication shall remain unalterable.	FDP_ACC.2 FDP_ACF.1
Chapter 4.5	**Audit**	
Chapter 4.5	The TOE must monitor events that indicate a potential violation of its security. Assignment (FAU_SAA.1.2) Subset of defined auditable events:	FAU_SAA.1

	- cardholder authentication failure (5 consecutive unsuccessful PIN checks), - self test error, - stored data integrity error, - activity data input integrity error.	
Chapter 4.6	**Accuracy**	
Chapter 4.6.1 4.6.2	Stored data integrity Assignment (FDP_SDI.2.2) Actions to be taken: warn the entity connected, Basic data authentication Assignment (FDP_DAU.1.1) List of objects or information types: activity data. Assignment (FDP_DAU.1.2) List of subjects: any.	FDP_SDI.2 FDP_DAU.1
Chapter 4.7	**Reliability**	
Chapter 4.7.1	Tests Selection (FPT_TST.1.1): during initial start-up, periodically during normal operation. Note: during initial start-up means before code is executed (and not necessarily during Answer To Reset procedure).	FPT_TST.1
RLB_301	The TOE's self tests shall include the verification of the integrity of any software code not stored in ROM.	FPT_TST.1
RLB_302	Upon detection of a self test error the TSF shall warn the entity connected.	FPT_TST.1
RLB_303	After OS testing is completed, all testing-specific commands and actions shall be disabled or removed. It shall not be possible to override these controls and restore them for use. Command associated exclusively with one life-cycle state shall never be accessed during another state.	FPT_TST.1
Chapter 4.7.2 RLB_304	There shall be no way to analyse, debug or modify TOE's software in the field.	FIA_USB.1 FPR_UNO.1 FPT_EMS.1 FPT_PHP.3 ADV_ARC (self-protection for

		stored data)
RLB_305	Inputs from external sources shall not be accepted as executable code.	FDP_ITC.1 FIA_USB.1
Chapter 4.7.3 RLB_306	The TOE shall preserve a secure state during power supply cut-off or variations.	FDP_RIP.1 FPT_FLS.1
Chapter 4.7.4 RLB_307	If power is cut (or if power variations occur) from the TOE, or if a transaction is stopped before completion, or on any other reset conditions, the TOE shall be reset cleanly.	FDP_RIP.1 FPT_FLS.1
Chapter 4.8	**Data Exchange**	
Chapter 4.8.1 DEX_301	The TOE shall verify the integrity and authenticity of data imported from a Vehicle Unit.	FPT_TDC.1 FTP_ITC.1
DEX_302	Upon detection of an imported data integrity error, the TOE shall: - warn the entity sending the data, - not use the data.	FPT_TDC.1 FTP_ITC.1
DEX_303	The TOE shall export user data to the Vehicle Unit with associated security attributes, such that the Vehicle Unit will be able to verify the integrity and authenticity of data received.	FPT_TDC.1 FTP_ITC.1
Chapter 4.8.2 DEX_304	The TOE shall be able to generate an evidence of origin for data downloaded to external media.	FCO_NRO.1 FDP_ETC.2
DEX_305	The TOE shall be able to provide a capability to verify the evidence of origin of downloaded data to the recipient.	FCO_NRO.1 FDP_ETC.2
DEX_306	The TOE shall be able to download data to external storage media with associated security attributes such that downloaded data integrity can be verified.	FCO_NRO.1 FDP_ETC.2
Chapter 4.9	**Cryptographic support**	
CSP_301	If the TSF generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key	FCS_CKM.1 FCS_CKM.4

	sizes. Generated cryptographic session keys shall have a limited (TBD by manufacturer and not more than 240) number of possible use.	
CSP_302	If the TSF distributes cryptographic keys, it shall be in accordance with specified cryptographic key distribution methods.	FCS_CKM.2

Table 8: Coverage of the GST [8] requirements

272 Furthermore, the Threats and Security Objectives described in chapters 3.3, 3.4 and 3.5 of [8] are identical to the corresponding Threats and Security Objectives defined in sec. 3.2 and 4.1 of the current PP. Because the personalisation and the secure handling of cryptographic material are important for the TOE security the PP considers the additional threat T.Personalisation_Data which was not in focus of [8]. The corresponding security objectives for the TOE environment is considered in the current PP too.

273 So, since the threats and security objectives of the GST [8] and this PP are identical and all requirements of the GST [8] are addressed by the current PP, it can be stated that the current PP covers the GST [8] completely.

10 Annex B: Functional Tests

274 This Annex B contains information concerning the functional tests of the Tachograph Cards and gives an overview of the test range. It is useful for the Tachograph Card evaluation preparation, but it is not required to reflect this information in the corresponding Security Targets.

275 The Appendix 9 of the [5] specifies the necessary functional tests which are listed here for the sake of completeness:

Command	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

Table 9: List of functional tests

276 It is required to test the normal processing and the error messages for each of the listed commands.

For normal processing:

277
- test at least once each allowed usage of each commands (ex: test the UPDATE BINARY command with CLA = '00', CLA = '0C' and with different P1, P2 and LC parameters)

279
- check that the operations have actually been performed in the card (ex: by reading the file the command has been performed on)

280 All requirements (TCS 313 – TCS 379) of the Tachograph Card specification [8] have to be tested.

For error messages:

281
- test at least once each error message (as specified in the [7]) for each command and

282
- test at least once every generic error (except '6400' integrity errors checked during security certification.